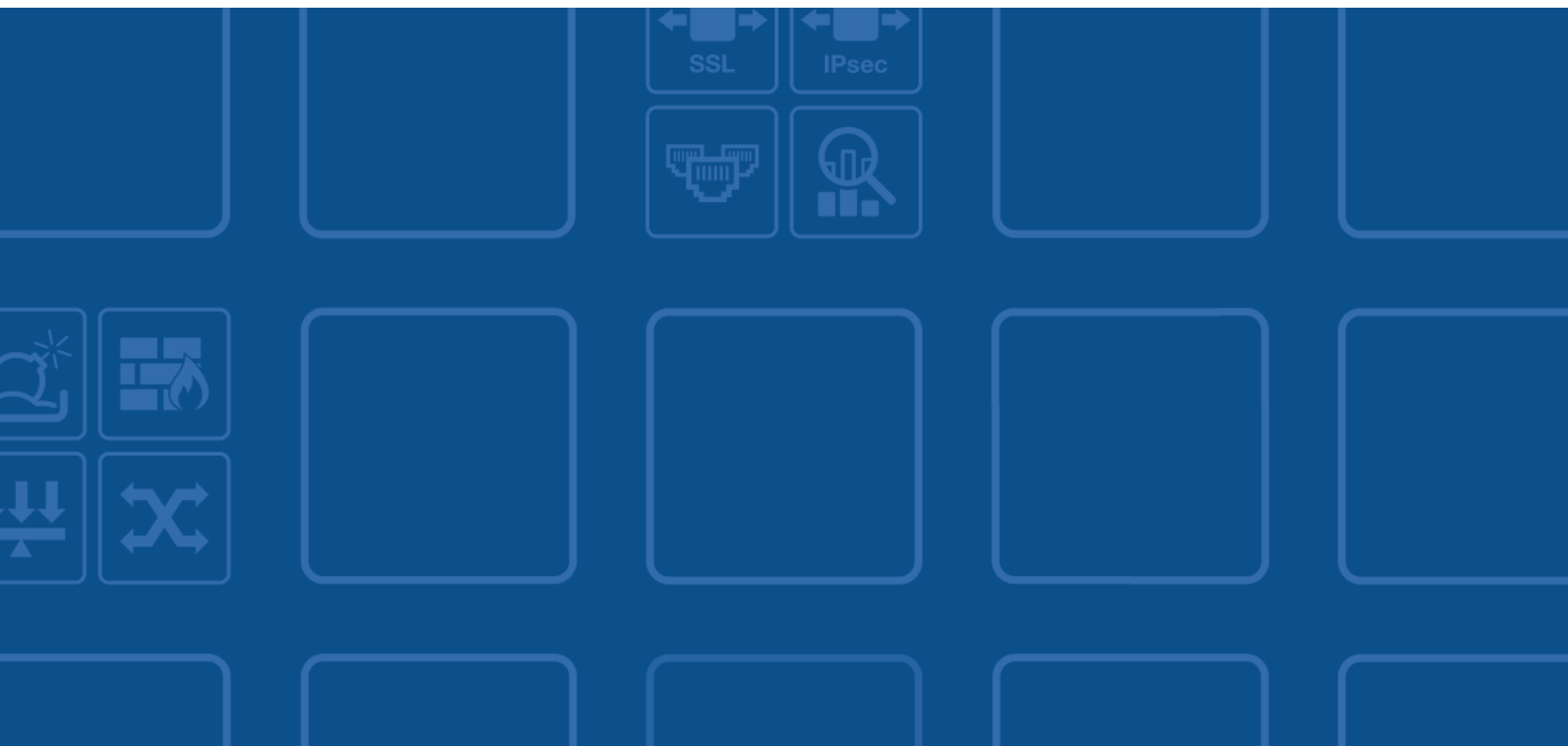
FORTINET
High Performance Network Security

FortiClient (Android) - User Guide

VERSION 5.4.0



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

September 16, 2016

FortiClient (Android) 5.4.0 User Guide

04-540-385156-20160916

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-09-16	Initial release of 5.4.0.

Introduction

FortiClient (Android) 5.4 includes support for IPsec VPN, SSL VPN, Web Security, Endpoint Control, and FortiClient Enterprise Management Server (EMS).

FortiClient (Android) 5.4 features

The following table lists and describes features supported in FortiClient (Android) 5.4.

Feature	Description
IPsec VPN	• Configure IPsec VPN connections. • IKE main mode and aggressive mode support. • Client X.509 certificates and pre-shared key support. • Enable always up and auto connect options. • Disable auto start.
SSL VPN	• Configure tunnel mode SSL VPN connections. • Client and server X.509 certificates support. • Enable always up and auto connect options. • Disable auto start.
Web Security	• Allow or deny web browsing based on FortiGuard groups and categories. • Monitor web browsing violations • Client Web Filtering when On-Net.
Endpoint Control	• Registration to FortiGate and connection to FortiClient EMS • FortiTelemetry Gateway IP list • Provision of web filtering profile • Provision of VPN connections • Deployment of CA certificate • Disable unregister • User profile picture (Avatar)

Download FortiClient (Android) 5.4.0

You can download the FortiClient (Android) 5.4.0 application from the Google play application or at the following link: https://play.google.com/store.

Product Integration and Support

FortiClient (Android) 5.4.0 support

The following table lists FortiClient (Android) 5.4.0 product integration and support information.

Android operating systems	• 4.1 Jelly Bean (API level 16) • 4.2 Jelly Bean (API level 17) • 4.3 Jelly Bean (API level 18) • 4.4.3 KitKat (API level 19) • 4.4.4 KitKat (API level 20) • 5.0.1 Lollipop (API level 21) • 5.1.1 Lollipop (API level 22) • 6.0.0 Marshmallow (API 23) • 7.0.0 Nougat (API 24)
FortiOS	• 5.0.5 and later • 5.2.0 and later • 5.4.0 and later
FortiToken Mobile	• 3.0.0 and later For more information, see the FortiToken Mobile User Guide for Android.
FortiClient EMS	• 1.0.0 and later

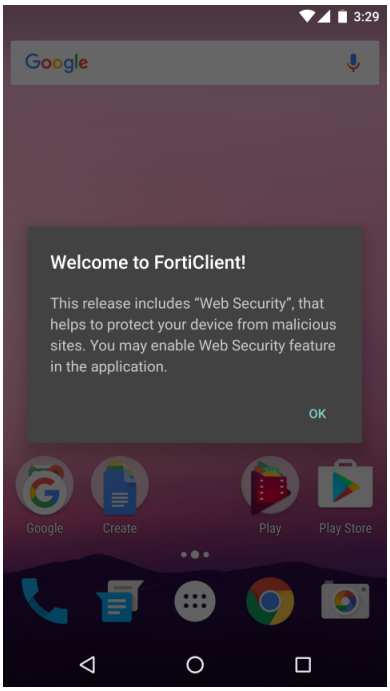
Open the Application

Open for the first time

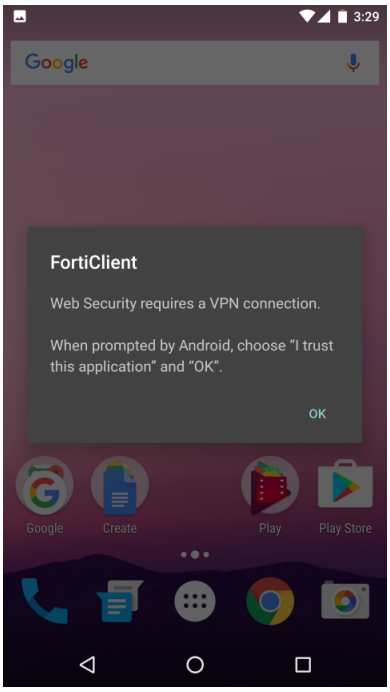
FortiClient (Android) includes a Web Security feature to help protect your device from malicious sites. When opening FortiClient, you will be prompted to enable the Web Security feature as well as respond to several questions. After that, FortiClient (Android) will automatically start when Android OS starts.

To open for the first time:

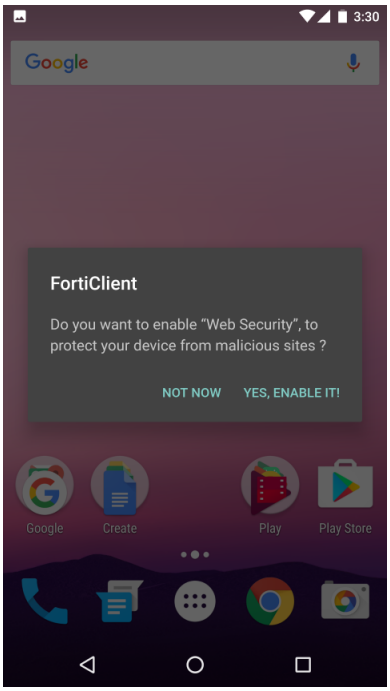
1. When you open FortiClient (Android), the *Welcome to FortiClient!* page is displayed. Click *OK*.



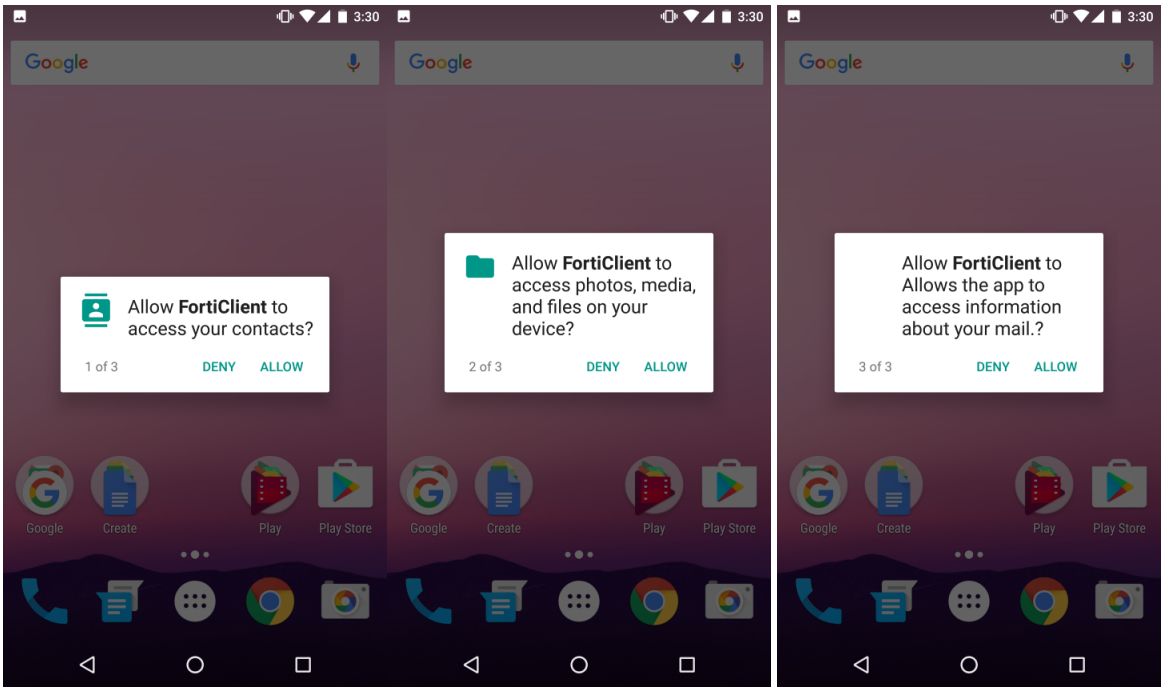
2. Information about requiring a VPN connection for web security is displayed. Click *OK*.



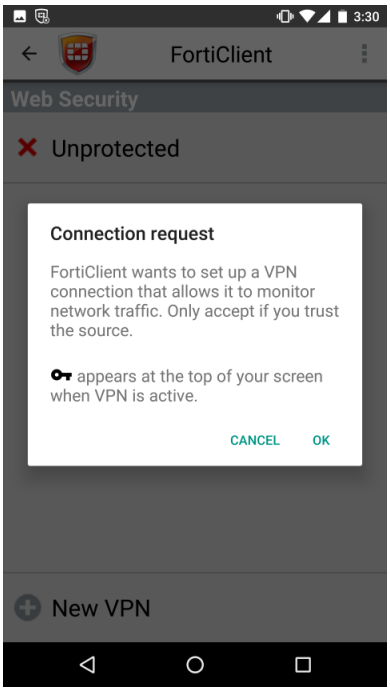
3. Information about enabling web security is displayed. Click *OK*.



4. Depending on the Android operating system, you may see the following pop-ups about permissions. Select *Allow*.



5. The *Connection request* page is displayed. Click *OK*.

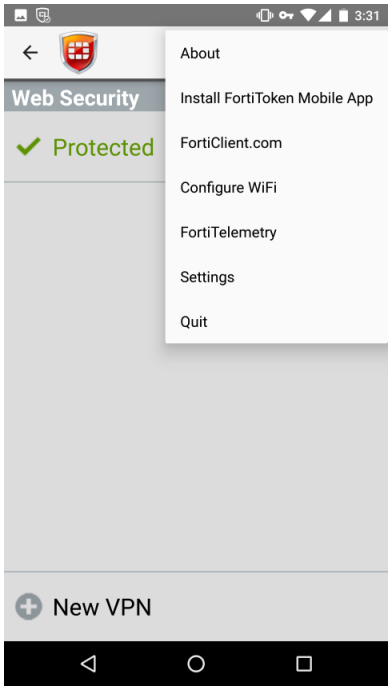


Launch from notification bar

FortiClient (Android) 5.4 allows you to launch the application from the notification bar.

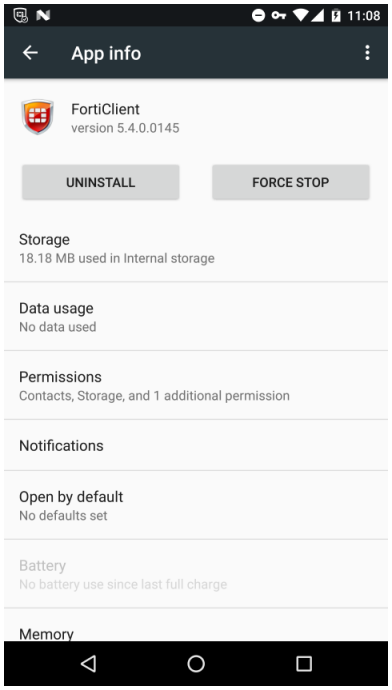
Quit from the app menu

You can quit the app from the menu page.



Force stop from the Apps page

When the Web Security feature is enabled, FortiClient (Android) runs in the background to provide the service. To quit the application, go to the Android OS Settings page, select *Apps*, select *FortiClient*, and select *Force stop*. On this page you can also clear data and uninstall FortiClient (Android).



Web Security

FortiClient (Android) 5.4 includes a web security feature to allow you to control web browsing on your Android device. You can select to allow or deny sites based on the FortiGuard site rating. The following table lists the web security groups and categories.

You can get up-to-date groups and categories from FortiGuard (http://www.fortiguard.com/static/webfiltering.html).

Groups	Categories
Security Risk	Malicious Websites, Phishing, Spam URLs
Potentially Liable	Drug Abuse, Hacking, Illegal or Unethical, Discrimination, Explicit Violence, Extremist Groups, Proxy Avoidance, Plagiarism, Child Abuse
Adult/Mature Content	Alternative Beliefs, Abortion, Other Adult Materials, Advocacy Organizations, Gambling, Nudity and Risque, Pornography, Dating, Weapons (Sales), Marijuana, Sex Education, Alcohol, Tobacco, Lingerie and Swimsuit, Sports Hunting and War Games
Bandwidth Consuming	Freeware and Software Downloads, File Sharing and Storage, Streaming Media and Download, Peer-to-peer File Sharing, Internet Radio and TV, Internet Telephony
General Interest - Business	Finance and Banking, Search Engines and Portals, General Organizations, Business, Information and Computer Security, Government and Legal Organizations, Information Technology, Armed Forces, Web Hosting, Secure Websites, Web-based Applications
General Interest - Personal	Advertising, Brokerage and Trading, Games, Web-based Email, Entertainment, Arts and Culture, Education, Health and Wellness, Job Search, Medicine, News and Media, Social Networking, Political Organizations, Reference, Global Religion, Shopping and Auction, Society and Lifestyles, Sports, Travel, Personal Vehicles, Dynamic Content, Meaningless Content, Folklore, Web Chat, Instant Messaging, Newsgroups and Message Boards, Digital Postcards, Child Education, Real Estate, Restaurant and Dining, Personal Websites and Blogs, Content Servers, Domain Parking, Personal Privacy
Unrated	Unrated

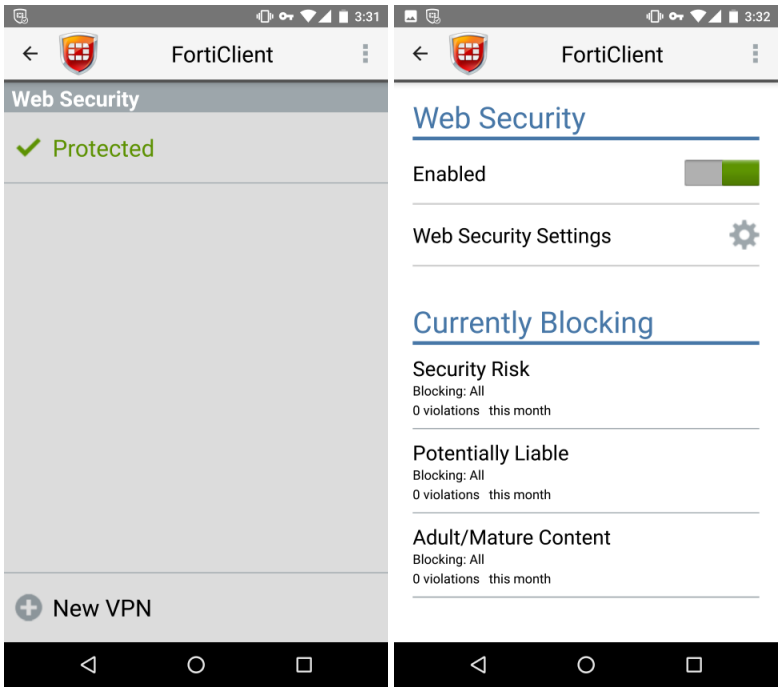
The Web Security module is only available in the full FortiClient (Android) app.

Provisioning of a web-filter exclusion list is only available from FortiClient EMS or FortiGate. Exclusion lists can only be applied on the domain name, not the full URL.

For more information on FortiGuard groups and categories, see http://www.fortiguard.com/static/webfiltering.html.

Web security status

The web security status will display *Protected* or *Unprotected*. When this feature is enabled, select *Protected* to view the blocked categories and the number of violations this month.



Enable and disable web security

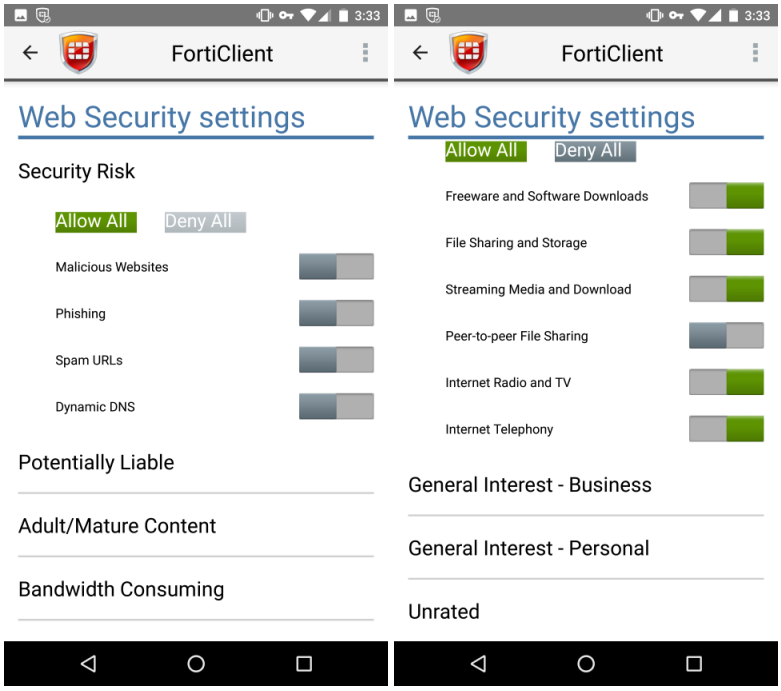
To enable web security, select *Unprotected*, then toggle the *Disabled* switch to *On*. To disable web security, toggle the *Enabled* switch to *Off*.

When FortiClient is managed by FortiGate Endpoint Control, the user cannot enable or disable web security.

Web security settings

To change web security settings, select Web Security Settings. There are seven top level groups with various categories. When you select a top level group a drop-down menu will appear. You can select to *Allow All*, *Deny All*, or select to allow or deny each category independently.

When FortiClient is managed by FortiGate Endpoint Control, the web security setting is deployed from FortiGate, and the user cannot change it.



When browsing to a website which falls into a category which is denied, you will receive a web page blocked page.


3:33
www.888.com/index.html
Web Page Blocked!
You have tried to access a web page which belongs to a category that is blocked.

SSL VPN

FortiClient (Android) 5.4 supports tunnel mode SSL VPN connections. You can either configure the SSL VPN in the FortiClient user interface or provision SSL VPN connections in an endpoint profile from FortiClient EMS. FortiClient EMS pushes provisioned SSL VPN configurations to your Android device after the FortiClient (Android) successfully registers with FortiGate for Endpoint Control and with FortiClient EMS for provisioning and monitoring.

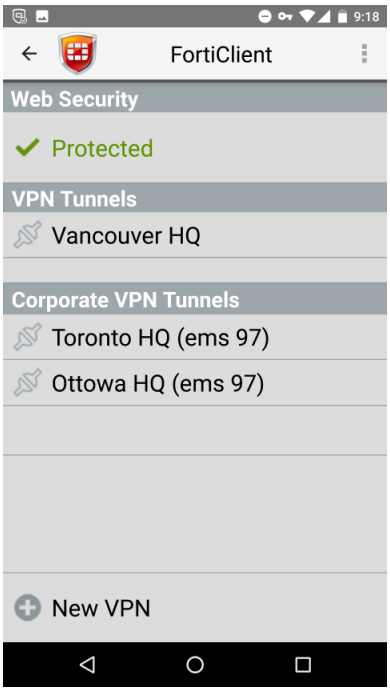
You can configure X.509 certificates, CA server certificates, and check server certificates. You can also configure always up and auto connect for the VPN connection.

Create an SSL VPN connection

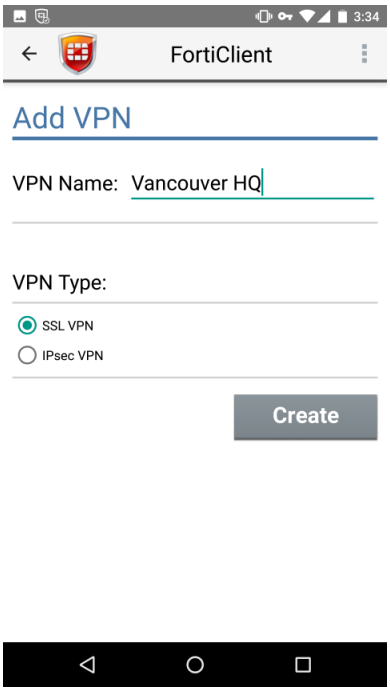
To create a new SSL VPN connection in the FortiClient (Android) user interface follow the steps listed below.

To create a new SSL VPN connection:

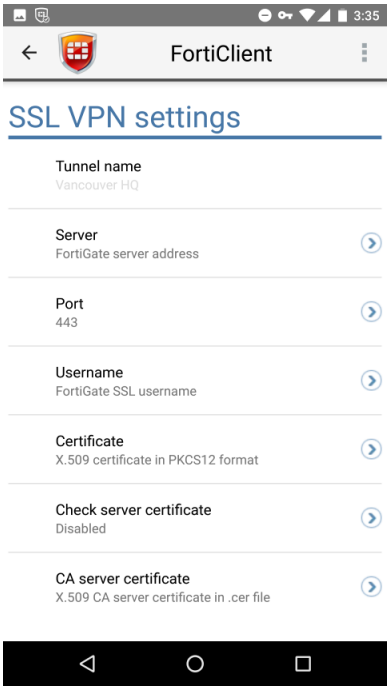
1. Select *New VPN* from the toolbar in the bottom of the page.



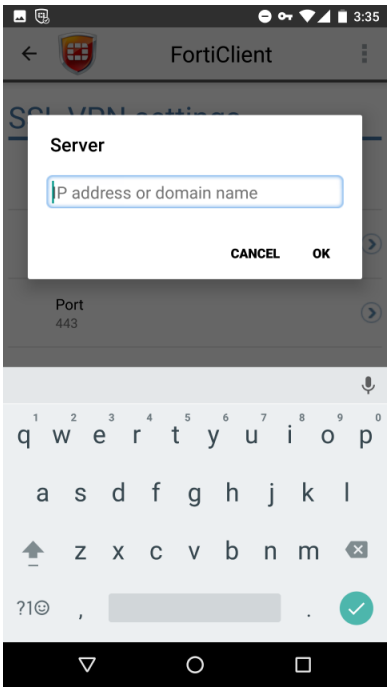
2. Enter a name for the new VPN connection, select *SSL VPN* under *VPN Type*, and select *Create*.



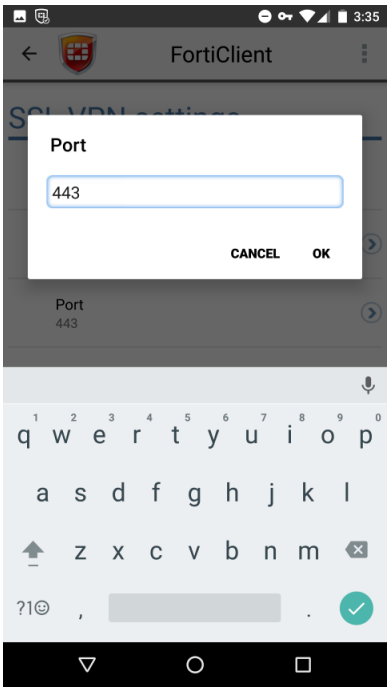
The SSL VPN settings page is displayed.



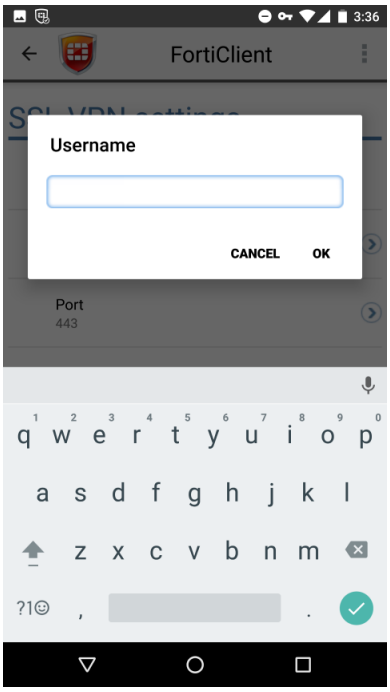
3. Select *Server*, enter the server IP address or domain name, and select *OK*.



4. Select *Port*, enter the port number, and select *OK*. The default port is 443.



5. Select *Username*, enter a user name, and select *OK*.

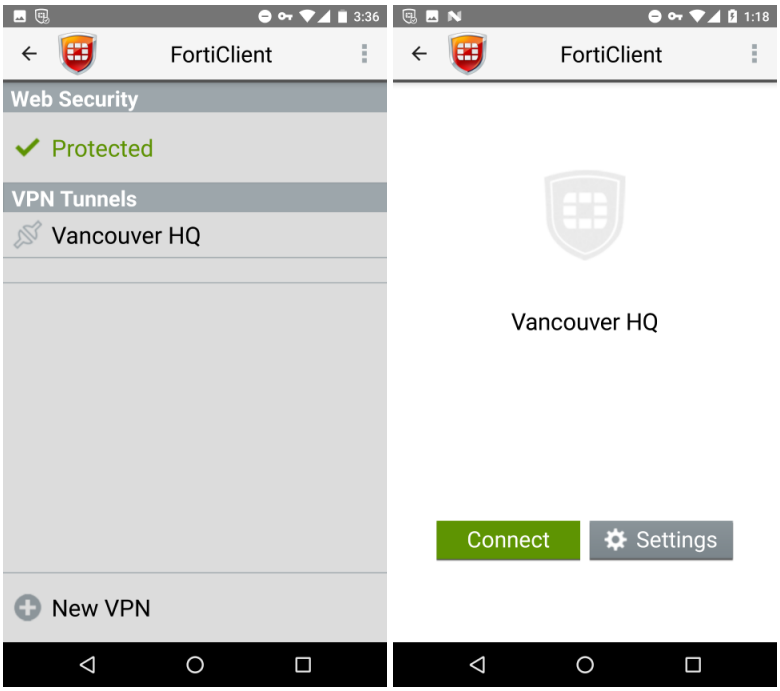


Connect to the VPN

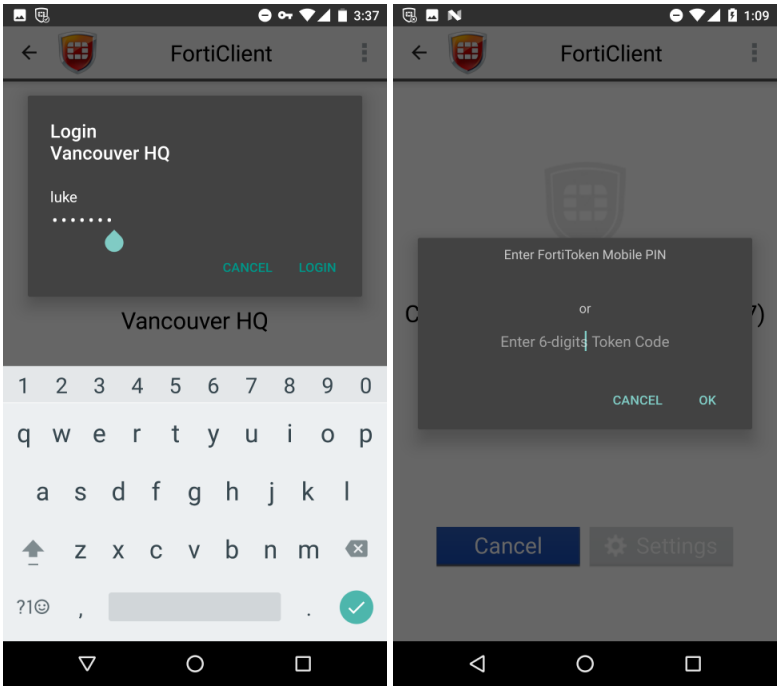
SSL VPN tunnel mode uses X.509 Certificates (PKCS12 format) for authentication. Certificate settings need to be configured if authentication requires the client certificate, otherwise leave the certificate settings as their default value.

To connect to the SSL VPN:

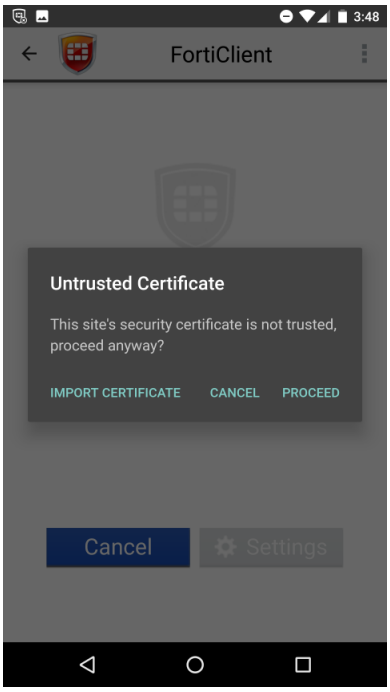
1. Select an available VPN and then select *Connect*.



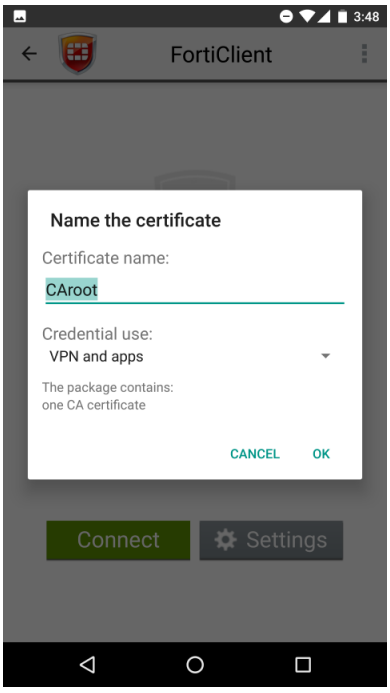
2. Enter your username and password and then select *Login*.



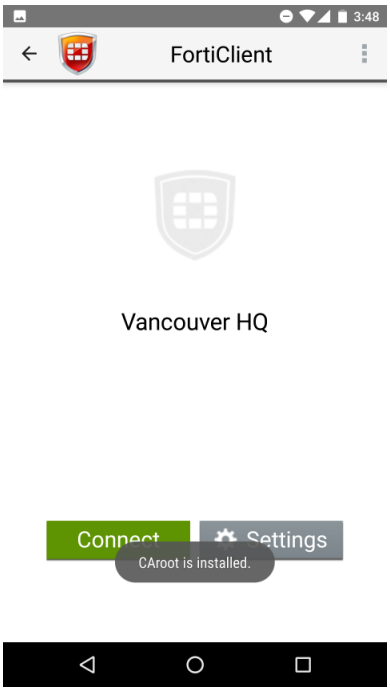
If the SSL VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token.



3. You will receive an *Untrusted Certificate* message dialog box warning message, and you will have the option to *Proceed*, *Cancel*, or *Import certificate*.



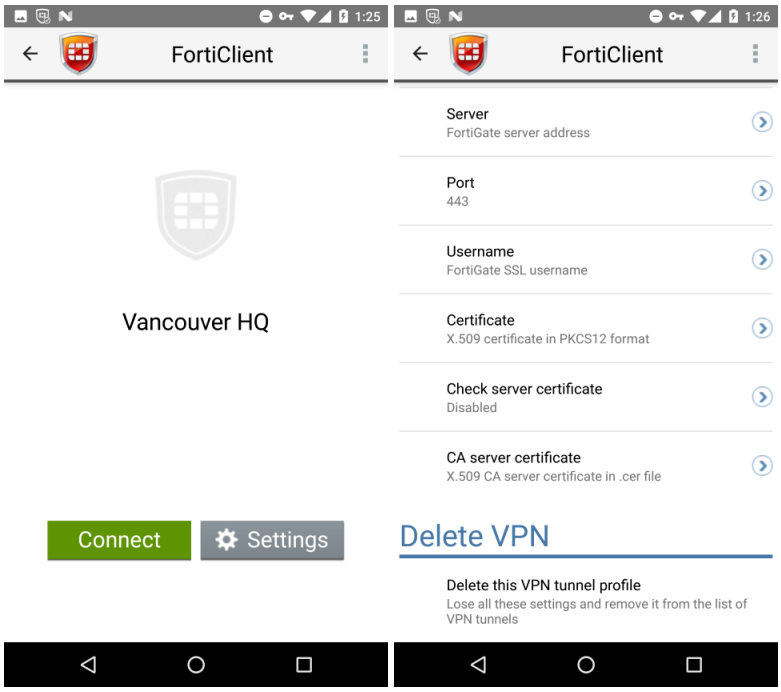
4. Select *Import certificate*, browse for the certificate file, edit the name (if required).



5. Select *OK* to load and install the certificate. The certificate is now installed on the device. Use the device back button to return to the connection screen.
6. Select an available VPN to connect.

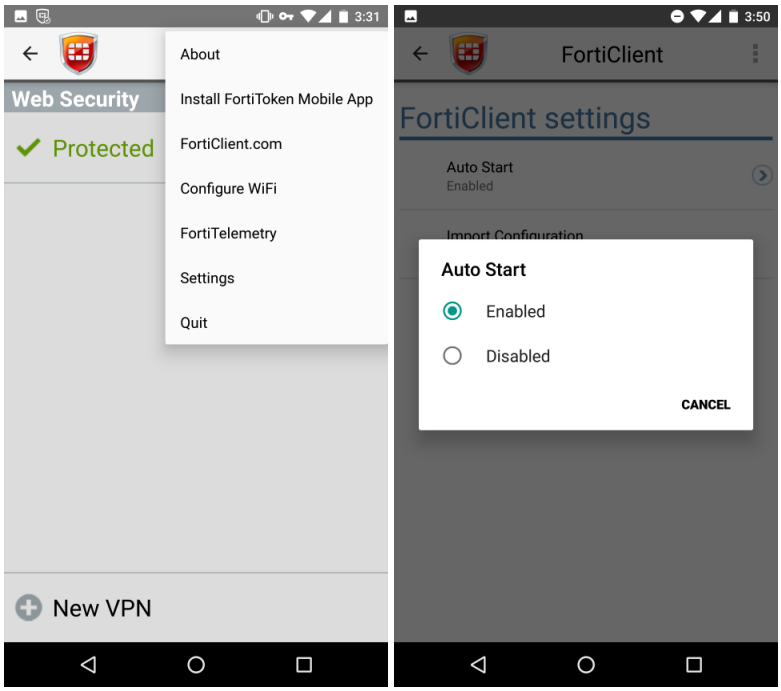
Edit SSL VPN settings or delete a SSL VPN configuration

To edit SSL VPN settings or delete an existing SSL VPN configuration, select the SSL VPN, and select the *Settings* button.



Auto start

You can enable or disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Settings* in the drop-down menu. In the FortiClient settings page select *Auto Start* and select *Enabled* or *Disabled*.



IPsec VPN

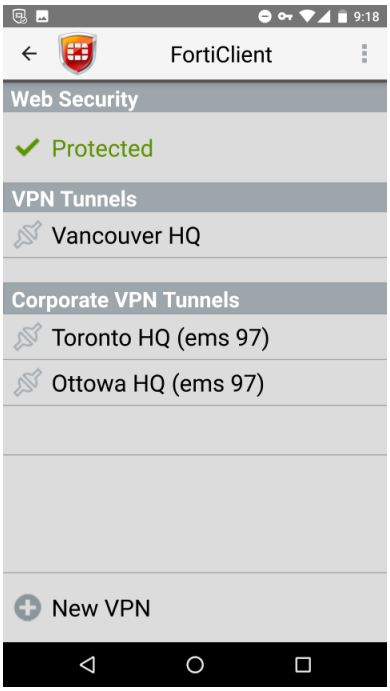
FortiClient (Android) 5.4 supports IPsec VPN connections. You can either configure the IPsec VPN in the FortiClient user interface or provision SSL VPN connections in an endpoint profile from FortiClient EMS. FortiClient EMS pushes provisioned SSL VPN configurations to your Android device after the FortiClient (Android) successfully registers with FortiGate for Endpoint Control and with FortiClient EMS for provisioning and monitoring.

You can configure server settings, phase 1, phase 2, and XAuth settings.

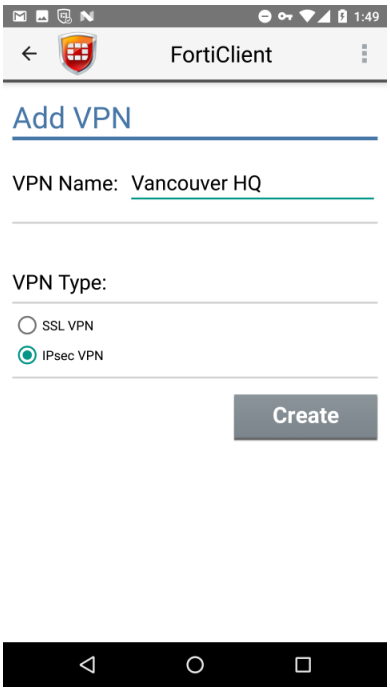
Create an IPsec VPN connection

Create a new IPsec VPN connection:

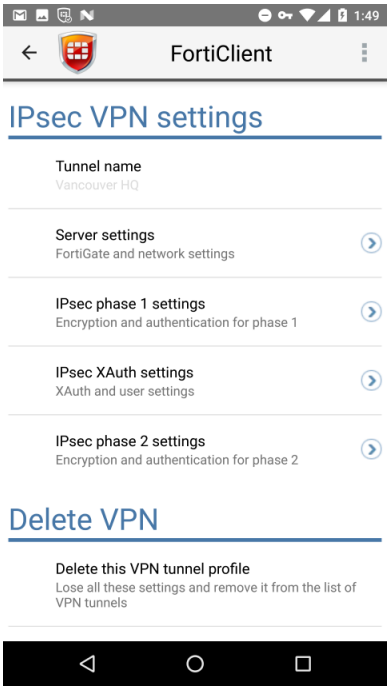
1. Select *New VPN* from the toolbar in the bottom of the page.



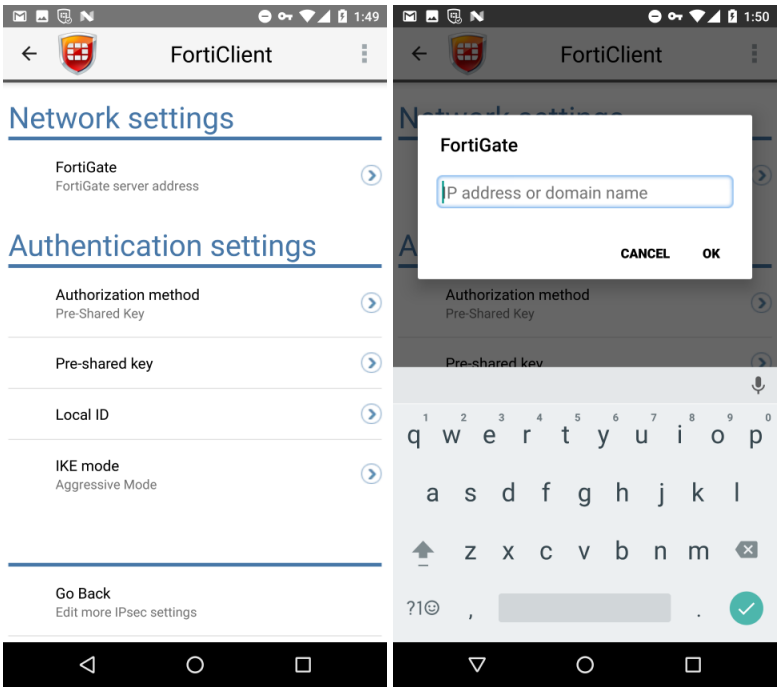
2. Enter a name for the new VPN connection, select *IPsec VPN* under *VPN Type*, and select *Create*.



The IPsec VPN settings page is displayed.



3. Select *Server settings* > *Network settings* > *FortiGate*. Enter the server IP address or domain name, and select *OK*.

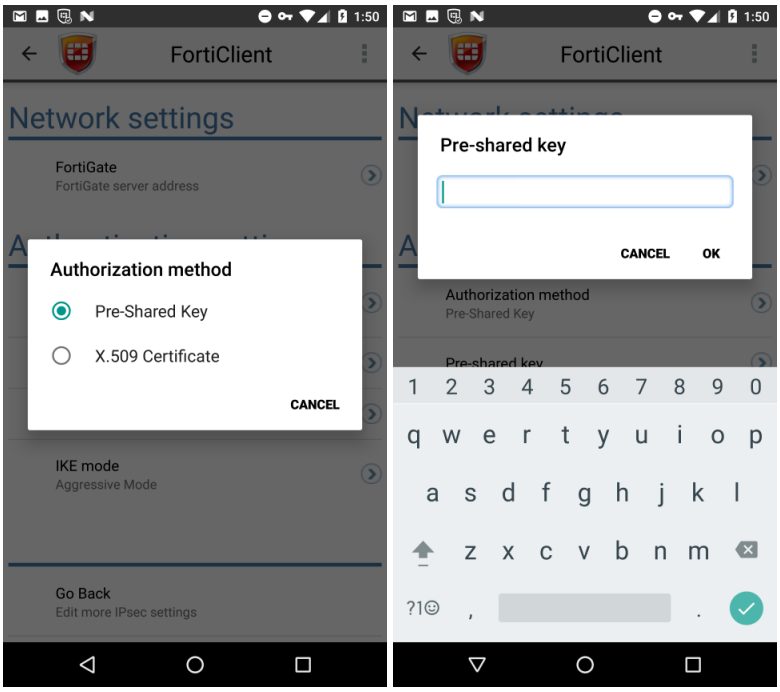


4. Under *Authentication*, select *Authorization method*, and select either *Pre-Shared Key* or *X.509 Certificate*.
5. For pre-shared key, select *Pre-shared Key* to enter the pre-shared key value.

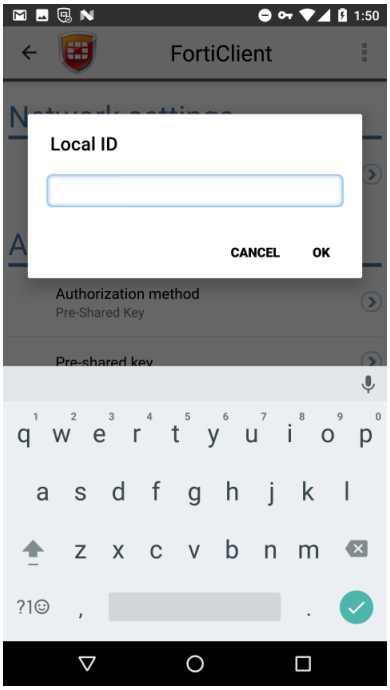
   The simplest way to authenticate with the FortiGate unit is by means of a pre-shared key. This is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth).

   The pre-shared key must contain at least 6 characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.

The pre-shared key configured on the client must match the pre-shared configured on the FortiGate. Contact your network administrator for the correct setting.



Select *Local ID*, enter the local ID, and select *OK*.

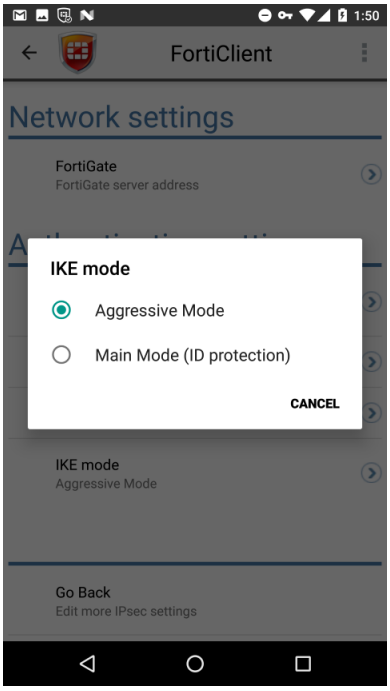


6. For X.509 certificate select *Certificate* and then browse for the certificate file on your device.

   To authenticate with the FortiGate unit using digital certificates, you must have the required certificates installed on the Android device (peer) and the FortiGate unit (server).

Contact your network administrator for the correct X.509 certificate file.

7. Select *IKE mode*, and select *Aggressive Mode* or *Main Mode (ID protection)*.



In *Aggressive Mode*, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

In *Main Mode*, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.

The *IKE Mode* selected on the client must match the mode selected on the server. Contact your network administrator for the correct setting.

8. Select *Go Back* to return to the *IPsec VPN settings* page.
9. Select *IPsec phase 1 settings* to view or edit the phase 1 proposal encryption and authentication settings. You can choose to use the default settings.

   Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

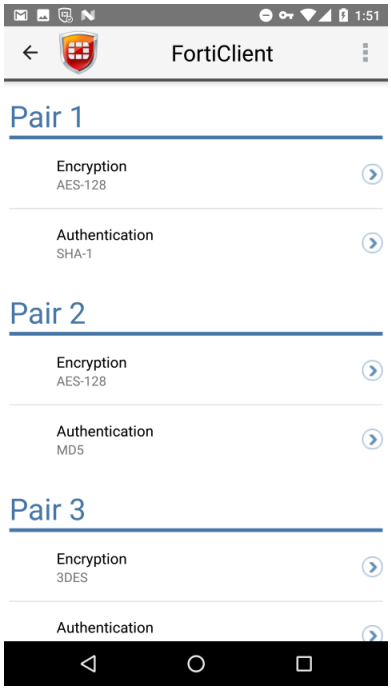
   - DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
   - 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
   - AES128: A 128-bit block algorithm that uses a 128-bit key.

   You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

   - MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
   - SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

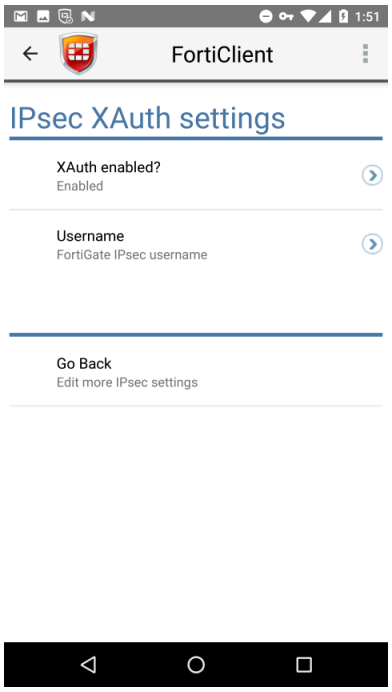
   Select one or more Diffie-Hellman (DH) groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.

Contact your network administrator for the correct phase 1 encryption and authentication algorithms, and DH group.



10. Select *Go Back* to return to the *IPsec VPN settings* page.
11. Select *IPsec XAuth settings* to view or edit the XAuth and user settings. XAuth is enabled by default. Select *Username* to enter the FortiGate IPsec username. Select *Password* to enter the password value. To use XAuth, you must first configure the user's credentials on your FortiGate, and external RADIUS or LDAP server.

    Extended authentication (XAuth) increases security by requiring the remote dialup client user to authenticate in a separate exchange at the end of phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS and LDAP to authenticate dialup clients.



12. Select *Go Back* to return to the *IPsec VPN settings* page.
13. Select *IPsec phase 2 settings* to view or edit the phase 2 encryption and authentication settings. You can choose to use the default settings.

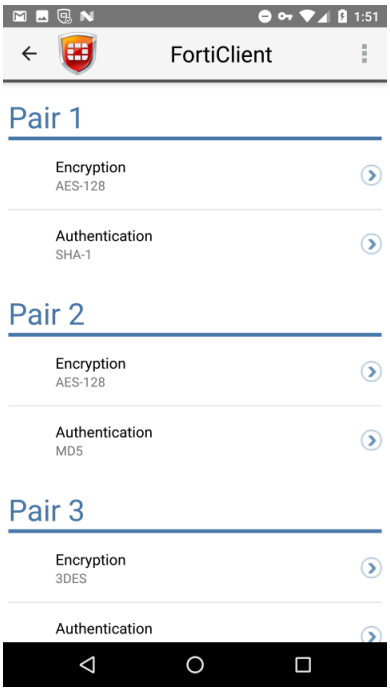
    Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

    - DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
    - 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
    - AES128: A 128-bit block algorithm that uses a 128-bit key.

    You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

    - MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
    - SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

    Select one or more Diffie-Hellman groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.



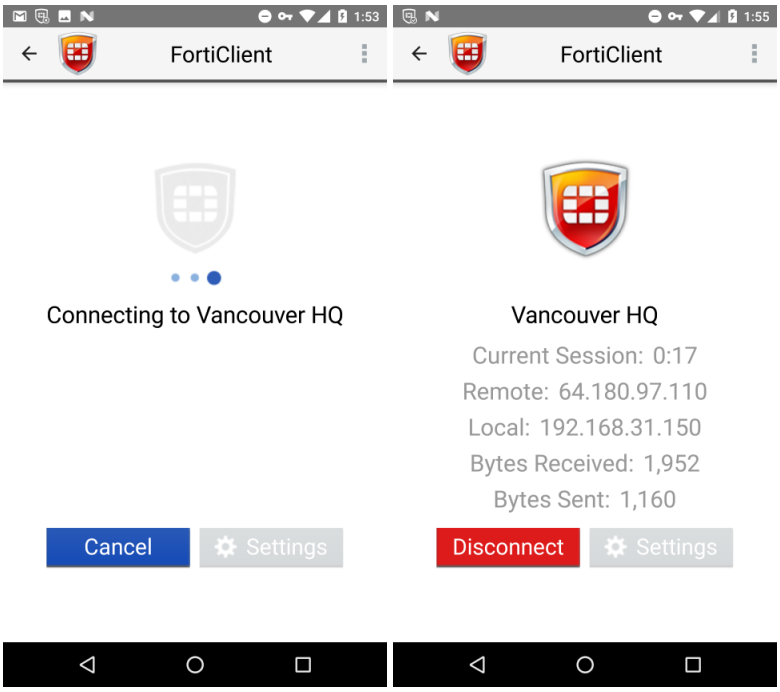
Contact your network administrator for the correct phase 2 encryption and authentication algorithms, and DH group.

14. Select *Go Back* to return to the *IPsec VPN settings* page.

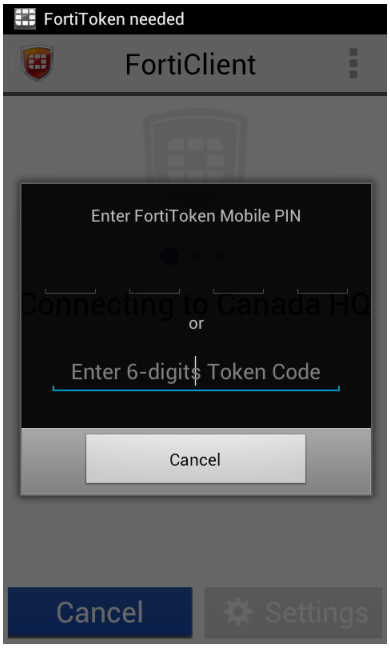
Connect to an IPsec VPN

Connect to an IPsec VPN:

1. Select an available IPsec VPN connection and then select *Connect*.
2. Enter the username and password, and select *Login*.

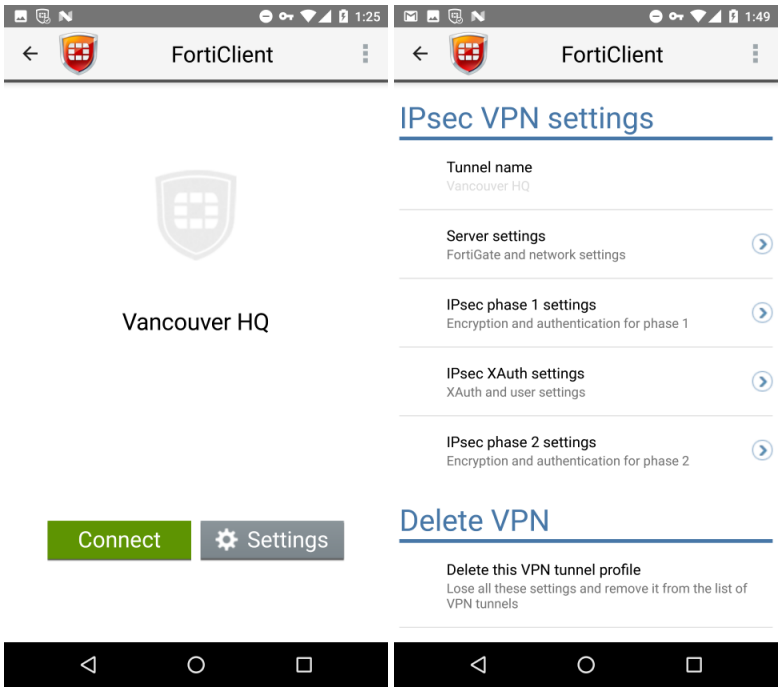


If the IPsec VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token code.



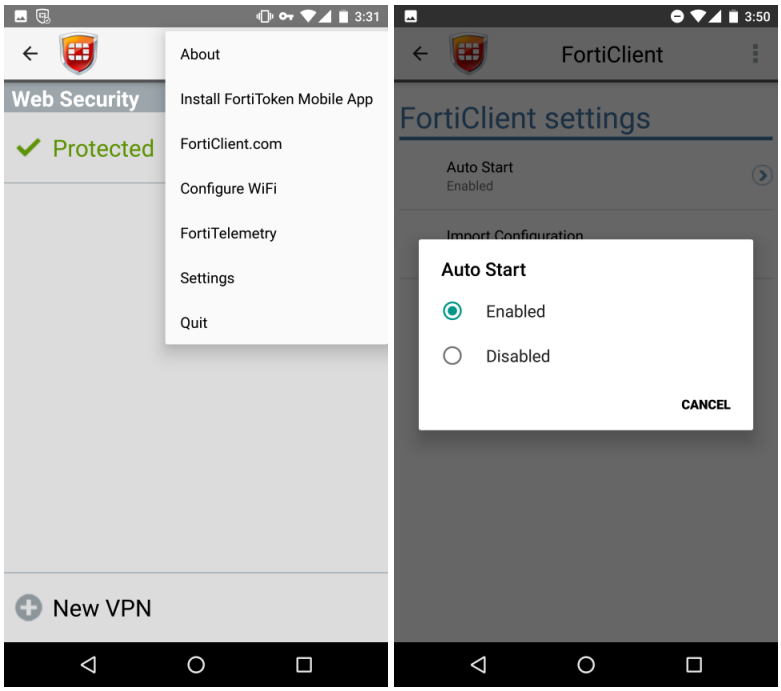
Edit VPN settings or delete a VPN configuration

To edit IPsec VPN settings or delete an existing IPsec VPN configuration, select the IPsec VPN, and select the *Settings* button.



Auto start

You can enable or disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Settings* in the drop-down menu. In the FortiClient settings page select *Auto Start* and select *Enabled* or *Disabled*.



Endpoint Control

FortiClient (Android) 5.4 allows you to register to a FortiGate device for Endpoint Control and connect to FortiClient EMS for provisioning and monitoring.

FortiClient EMS

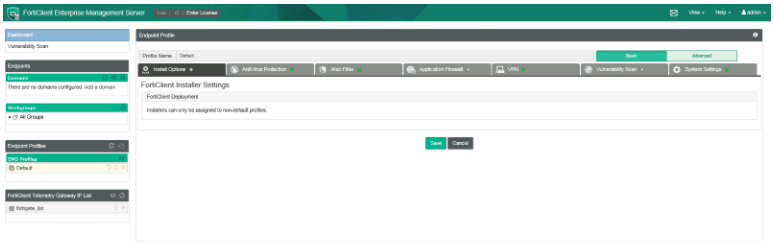
You use can use FortiClient EMS to create an endpoint profile and a FortiClient Telemetry Gateway IP list.

Configure FortiClient EMS Endpoint Profiles

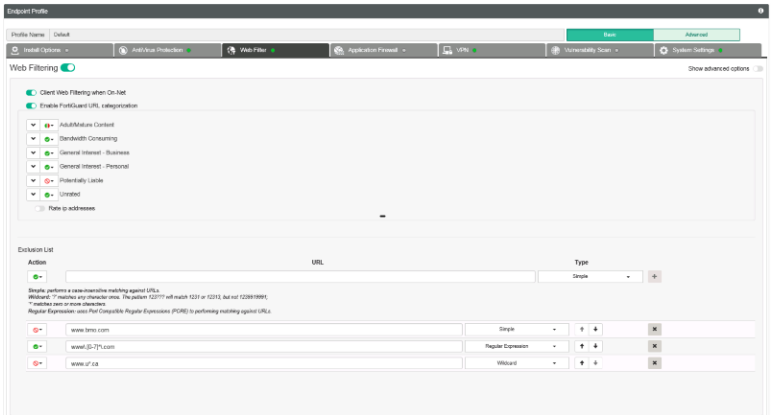
You can create a new endpoint profile or modify the default endpoint profile. The endpoint profile contains configuration information for FortiClient (Android), including VPN settings.

To configure FortiClient EMS endpoint profiles:

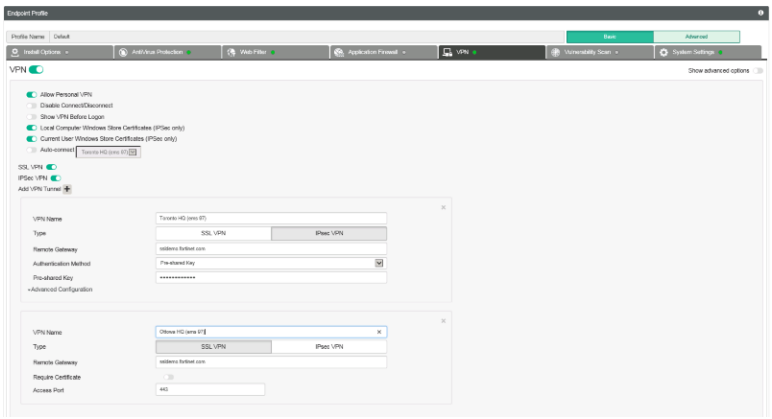
1. On FortiClient EMS, go to *Endpoint Profiles* > *Add a new profile*. The *Endpoint Profile* page opens.



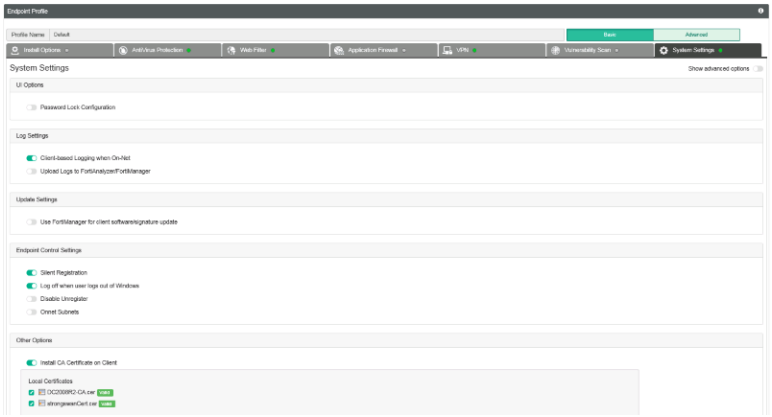
2. Click the *Web Filter* tab, and configure the settings.



3. Click the *VPN* tab, and configure the settings.



4. Click the *System Settings* tab, and select *Install CA Certificate to Client*.



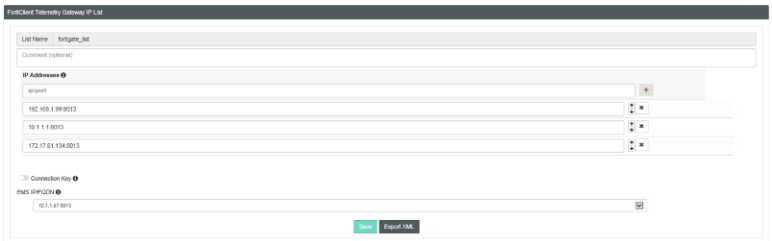
5. Select *Save* to save the settings.

Configure FortiClient Telemetry Gateway IP List

The FortiClient Telemetry Gateway IP list contains the IP address for one or more FortiGate devices and the IP address for FortiClient EMS. FortiClient (Android) can use the FortiClient Telemetry Gateway IP list to registration with a FortiGate device for Endpoint Control and connect to FortiClient EMS for provisioning and monitoring.

To configure FortiClient Telemetry Gateway IP lists:

1. On FortiClient EMS, go to *FortiClient Telemetry Gateway IP List*, and click the + button. The *FortiClient Telemetry Gateway IP List* page opens.



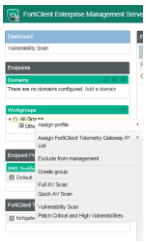
2. Configure the settings, and select *Save*.

Assign Endpoint Profiles and FortiClient Telemetry Gateway IP Lists

You must assign custom endpoint profiles and FortiClient Telemetry Gateway IP lists to domains or workgroups for them to be pushed to endpoints.

To assign endpoint profiles and FortiClient Telemetry Gateway IP lists:

1. On FortiClient EMS, go to *Workgroups*.
2. Right-click a domain or workgroup, and select *Assign profile* and then the profile. The profile is assigned to the domain or workgroup.

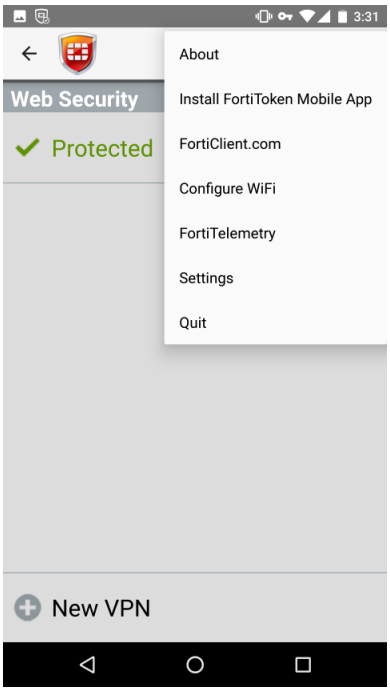


3. Right-click a domain or workgroup, and select *Assign FortiClient Telemetry Gateway IP List* and then the FortiClient Telemetry Gateway IP list. The FortiClient Telemetry Gateway IP list is assigned to the domain or workgroup.

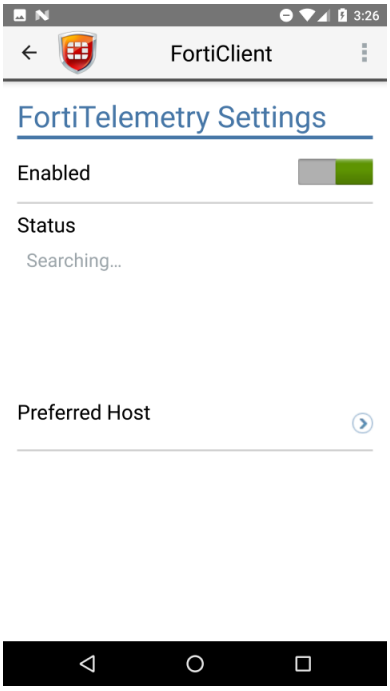
Register to FortiGate

Register to FortiGate:

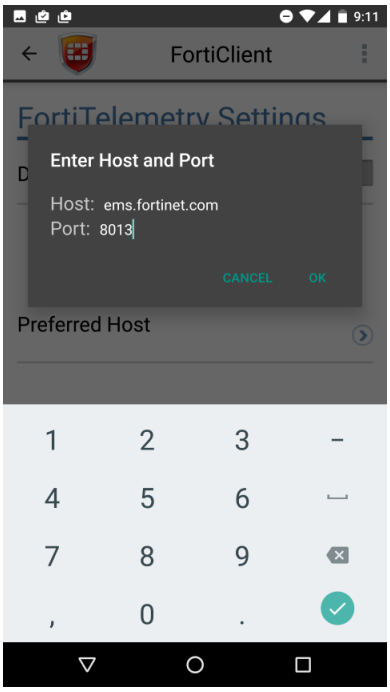
1. On your Android device, open the FortiClient application.
2. Select the menu icon in the toolbar and select *FortiTelemetry*.



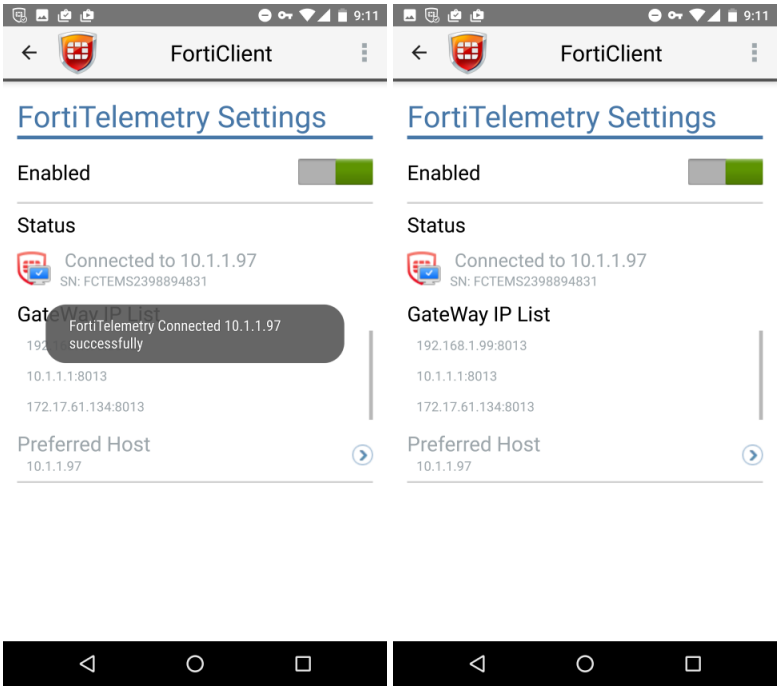
FortiClient searches for available FortiGate devices that are listed in the FortiClient Telemetry Gateway IP list. When FortiClient (Android) uses the FortiTelemetry settings to register to a FortiGate device, FortiClient (Android) also connects to FortiClient EMS and receives a profile from FortiClient EMS.



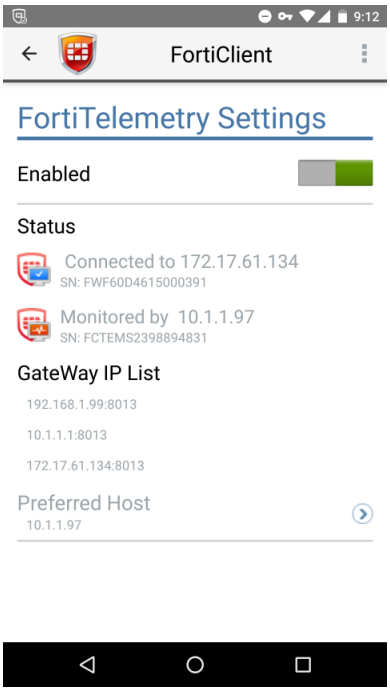
3. If FortiClient cannot locate a FortiGate device, you can select *Preferred Host* and enter the FortiGate host IP and port number.



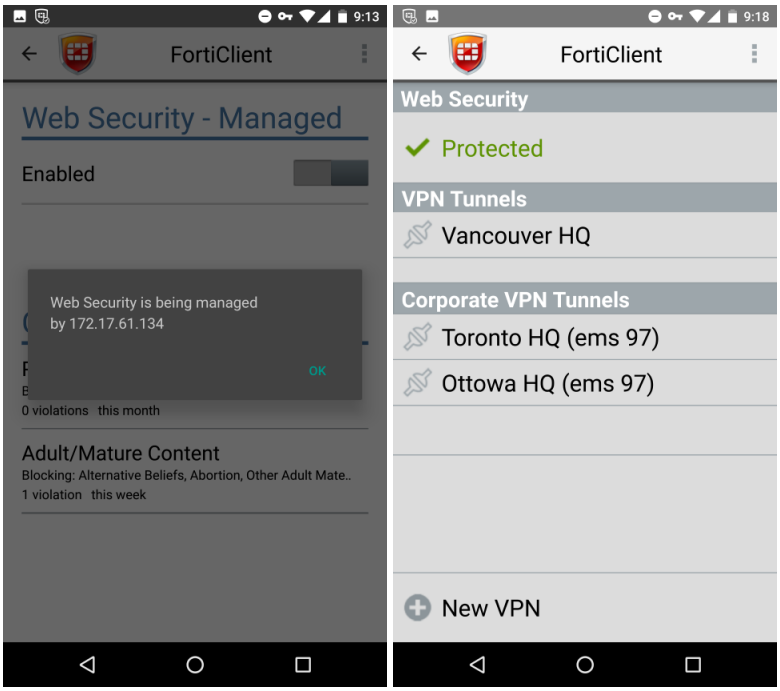
4. When a FortiGate is discovered you will receive a confirm registration dialog box with the FortiGate serial number and IP address. Depending on the FortiGate configuration, you may be required to enter a FortiClient registration key.



5. You will receive a confirmation dialog box when registration to FortiGate is complete.



6. Upon successful registration with FortiGate, FortiClient (Android) will receive the profile. The following image provides an example of a registered FortiClient (Android) with Web Category Filtering and provisioned VPN connections.

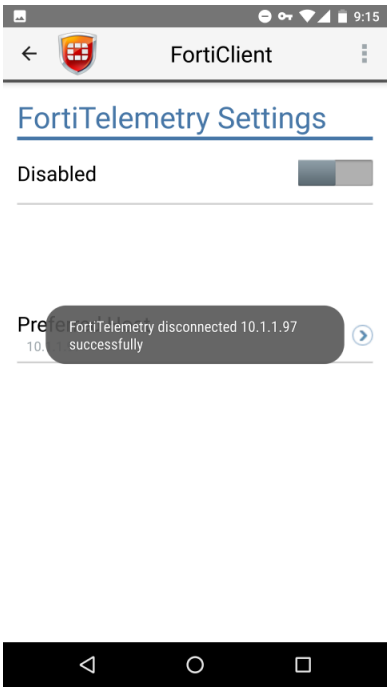


If FortiClient (Android) is registered to FortiGate, it will auto start when the phone is turned on and bring up the GUI.

Unregister from FortiGate

To unregister from FortiGate:

1. To unregister from FortiGate, in *Endpoint Control* settings page, in the *Status* section, select the close icon. You will receive a confirmation dialog box.



FORTINET®

High Performance Network Security